

Architectural & Engineering Specifications

Longwatch Video System
V5.0

www.longwatch.com

Longwatch Video System

General Specifications

The system shall support multiple types of communication infrastructures including internet, IP radios, leased lines, data radios, satellite, cellular, etc... and shall have the ability to work with any combination of these as part of the overall communication infrastructure.

The system shall support a set of distributed components (hardware and software) that allow for DVR recording “at the edge” along with event based alarming and automatic event based clip generation and notification. The system shall support for the deployment of four types of system components to meet the diverse nature of a highly distributed security system.

<u>Application</u>	<u>Infrastructure</u>	<u>Key Unique Requirements</u>
Remote Assets	Serial Radios (9600 baud), IP Radios, Cellular, Satellite, Frame Relay. Shared PLC/RTU protocols	1 or 2 Cameras Low Power = 9 Watts High Temp = -40 to 70(Deg C) 3 days built-in non-moving DVR storage (expandable) Event based alarm clip generation and operator notification Shared PLC/RTU protocols IPSec Security support SCADA Integration Access Control
Remote Facilities	Serial Radios (9600 baud), IP Radios, Cellular, Satellite, Frame Relay. Shared PLC/RTU protocols	Up to 6 IP Cameras 30 Days DVR storage (expandable) Event based alarm clip generation and operator notification Shared PLC/RTU protocols IPSec Security support SCADA Integration Access Control
Central Plants	LAN IP connection	Software DVR (runs on PC) Up to 12 Cameras 1280 by 1024 Resolution 30 frames per second Event based alarm clip generation and operator notification IPSec Security support SCADA Integration Access Control
Central Management Software	PC based Software. Supports multiple and diverse communication protocols for different remote types (see above)	Central Administration with remote configuration support. Centralized Event/Alarm database. Web based access to runtime and administration. Integrated Windows user security

Where an existing PLC data system is in use, the system shall support the ability to utilize the existing radio systems and /or lease lines used for remote PLC communications. This includes the ability to transmit video, access control management, PTZ camera control and configuration parameters over standard PLC protocols including Allen Bradley DF1, Modbus ASCII /RTU, Bristol Babcock BSAP, remote control systems. Where and when available, they system should be able to easily switch to support wireless IP connections such as cellular, IP radio, or IP satellite connections.

The video system shall consist of a distributed architecture of event based video surveillance components along with a centralized configuration and event management system. Video monitoring shall consist of a combination of remote video engines as well as one or more local plant video engines aggregated into a single comprehensive system for monitoring and viewing.

Each system shall support at least the following modes of video collection and transmission.

1. Live Streaming – of one or more selected remote cameras.
2. Guard Tour – ability to periodically sample and store all cameras in the system.
3. Video Event Clips – generates video clip based on event, capturing video before and after the event or for the duration of the event trigger.
4. Local DVR archival of at least 30 days or 3 to 5 days for the Micro Video Engine.

Each system shall support the ability to monitor for external events with up to 12 input sensors, to use direct built-in video motion analysis, or to utilize available events existing on supported cameras. When an event is detected, the system shall generate an event clip using configurable “before” and “after” times or “while active” time. The clip shall support up to 640 by 480 resolution and frame rates of up to 5 frames per second.

This event clip shall be automatically transmitted to a central system for storage, playback, and automatic user notification via email or phone. The system shall support “Store/Forward” capability; storing up to 32 event clips on the video engine in the event of communication loss as well as allowing for the connection to be lost during transfer of an event clip and have the download continue automatically and without operator interaction after the communication has been reestablished with no loss in video frames or quality.

The system shall provide centralized web-based configuration of all video collection devices with the ability to remotely download or upload new configuration parameters over the above listed communication infrastructures or PLC data systems.

The system shall provide a web-based interface for viewing of live feed video, event clip playback, DVR playback over TCP/IP networks and event historian access as well as full system configuration and deployment.

The system shall support live video viewing, event clip playback, and DVR video playback as well as full system configuration abilities through Microsoft Internet Explorer web browser ActiveX controls inserted into supporting applications for seamless integration.

The system shall provide open access and integration of video live feed, event clip playback,

DVR video playback and event historian access directly within a SCADA system's operator graphics page.

The system shall support an OPC Data Access server that would allow the integration of real-time status and security alarm information of all video capture devices into the HMI's alarming system. Furthermore, operator output actions such as goto preset, arm/disarm, and providing remote authorized entry shall be available by the HMI should this interface be utilized.

The system shall support a Modbus TCP server that would allow the integration of real-time status and security alarm information in the form of Modbus registers, of all remote video capture devices. Furthermore, operator output actions such as goto preset, arm/disarm, and providing remote authorized entry shall be available by the HMI should this interface be utilized.

The system shall support integration with third party access control systems and external user security panels to provide arming and disarming through hard wired inputs into the system via the provided I/O module, Modbus TCP Ethernet I/O devices or supported camera I/O. Inputs into the system shall have the ability to trigger an alarm and associated video clip as well as arming and disarming of individual alarm zones or the entire system.

The system shall have the ability to automatically trigger up to 4 outputs when an input is triggered to unlock doors/gates, turn on lighting, notify third party products, arm/disarm the system, etc....

The system shall support medium speed (19.2K to 512K bits/sec) IP based radio connections using TCP or UDP with sufficient error handling and bandwidth management to allow for up to 100 remote cameras. The system shall also support low speed (2400 Baud to 9600 Baud) Serial based radio connections using licensed or unlicensed frequencies or telephone dial out modems with sufficient error handling and bandwidth management.

The system shall support up to 9 serial HID based badge card readers supporting HID formatted access cards. Valid card access can trigger an output at the reader to unlock a door and additionally disarm an associated zone or the entire system.

The system shall support one numeric keypad that can be placed in or outside of the facility. The system shall support system and per user passwords that will arm or disarm individual alarm zones or the entire system.

The system shall support a two pass security verification mode where access to the facility would only be allowed if both a valid badge and badge specific password are entered.

The readers shall be able to trigger an alarm and associated video clip if a Bad Badge, Tamper Event, or Unauthorized Door Open event is detected.

The system shall support a centralized configuration and permissions control of all users and permissions. The system shall support automatic deployment of permissions and rights from the central system to all of the remotes and associated readers using the available communication channels outlined above.

The system shall support the granting of individual door/reader access permission as well as per user passwords with optional password expiration. The system shall support the on-line redeploy of permissions from the central system.

Readers and keypads are required to work in stand-alone mode as well as network mode. In the event that network communications is lost, the reader or keypad shall switch to stand-alone mode and perform local badge validation and door control.

The system shall support the remote monitoring and door operation remotely via a web page, as well as, integrated into an HMI using OPC Data Access or Modbus TCP servers.

The system shall support integrated PTZ operations via either a 485 multi-dropped PELCO-D communications line or directly to a PTZ enabled Axis IP camera.

The system shall support up to 9 named PTZ presets per camera. Any event (sensor, video analytic, camera event, reader event, keypad event) can be configured to automatically move one or more cameras to a specific preset to generate a video clip.

All PTZ camera operations shall allow remote and local control including (pan, tilt, zoom increments and goto preset operations). This operator control shall be supported through a web page, ActiveX control, or via OPC Data access or Modbus TCP servers.

The system shall support the integration of up to 12 IP cameras at each site. The system will perform all local storage, event detection, queuing, and live feed management of an IP camera in the same way it handles one of the 4 analog video inputs. That is, systems that will use IP cameras DO NOT require an IP connection between the Video Engine and the central station.

The system shall support any combination of analog or IP cameras up to a maximum of 12 total cameras per Video Engine.

The system shall allow for Axis IP camera events (DI, Motion, Audio, Tamper, or No Video signal) to generate a system alarm and trigger an event video clip.

The system shall support the ability to prevent access to the web based configuration by using Windows Integrated system security. That is, standard Windows domain or system user accounts shall be granted permission to configure the system. Any user without authorization will not be granted access to view or make changes to the system.

The system shall support optional 128 bit TCP Encryption between the central station and all remotes.

The system shall support the ability to publish an MJPEG video stream of any of the remote Video Engine's cameras to allow video integration into 3rd party in-plant security products.

The Local Video Engine shall consist of software and technology components that allow for video surveillance in a central plant facility. The system shall support one or more LVEs per Video Control Center. One or more LVE instances shall run on a separate PC and perform the collection, storage, and event monitoring of IP based video streams. These camera streams may come from IP cameras or video server components that convert analog video to IP video.

Each LVE instance shall support the same interface and capabilities of the Remote Video Engines (above) with the following additions:

1. LVE shall support up to 12 IP Cameras
2. Minimum of a total of 100 frames / sec per server (on a 2.4 Ghz Dual Pentium 4)
3. Minimum of 20 frames / sec per camera.
4. Archiving resolutions up to 1280 by 1024.
5. LVE supports up to 16 access control readers or keypads.
6. The LVE utilizes I/O built into Axis IP Cameras, access readers, access keypads, and external Modbus TCP I/O for event detection triggers.
7. LVE supports arm/disarm via the Video Control Center, SCADA system via OPC or Modbus TCP, reader card swipe, or keypad.
8. Support for Axis IP or IV&C Camera PTZ control.
9. Support event clip generation based on Axis IP camera video analytics detection.

Longwatch Video System Detailed Specifications

The video system shall be the Longwatch Video System. This video system is hereinafter referred to as the LVS.

1. The LVS shall incorporate the following hardware and software:
 - 1.1. Micro Video Engine (Micro) – integrated hardware and software unit for capturing and transmitting video streams and event data (located at extremely remote/low power locations).
 - 1.2. Remote Video Engine (RVE) – integrated hardware and software unit for capturing and transmitting video streams and event data (located at remote facilities)
 - 1.3. Local Video Engine (LVE) – integrated software for capturing and transmitting video streams and event data (located at remote facilities or central plants).
 - 1.4. Video Control Center (VCC) – software to manage configuration, monitor system data and share data with third party systems.
2. The RVE system shall incorporate the following operational features and characteristics:
 - 2.1. The RVE system shall provide the collection, analysis, and storage of video images at a remote location and not require a high speed connection to the remote site.
 - 2.2. The RVE system shall provide the following hardware characteristics.
 - 2.2.1. Support for 6 cameras (4 Analog Video Inputs).
 - 2.2.2. 12 Digital Inputs, 4 Digital Outputs.
 - 2.2.3. 1 Master Arm / Disarm Digital Input.
 - 2.2.4. Permanent storage of 250GB.
 - 2.2.5. RS232, USB, and Ethernet access ports.
 - 2.2.6. Optional (9) serial card reader.
 - 2.2.7. Optional keypad.
 - 2.3. The RVE system shall support the transfer of video, event, access control, and configuration information between the host VCC system and the RVE using the existing communications network supporting a bandwidth speed as low as 2400 baud. These networks could include but are not limited to,
 - 2.3.1. PLC Networks - Allen Bradley DF1, Modbus ASCII and RTU, Bristol Babcock BSAP.
 - 2.3.2. RS232 Connection – SIO.
 - 2.3.3. IP connections using TCP and UDP.

- 2.3.4. Dial out phone modems.
- 2.4. The RVE system shall provide 3 modes of video image collection.
 - 2.4.1. DVR Mode – local streaming video storage with the following minimum characteristics.
 - 2.4.1.1. Up to 30 days local video storage.
 - 2.4.1.2. Analog Resolution up to 640 by 480.
IP Camera Resolution up to 1280 by 1024.
 - 2.4.1.3. Analog capture up to 2 frames / sec capture for 4 cameras.
IP Camera capture up to 30 frames/sec for 6 cameras
 - 2.4.1.4. Windows media player compatible video file formats.
 - 2.4.1.5. IP Camera recording should support Audio archiving.
 - 2.4.2. Event Mode – Event clip generation around the detection of “security events”.
 - 2.4.2.1. Configurable WHILE ACIVE and BEFORE and AFTER time settings.
 - 2.4.2.2. Associate up to 4 independent camera clips per event.
 - 2.4.2.3. Activation of any of the 4 Digital Outputs.
 - 2.4.2.4. Local store and forward operation of the event and clips when VCC communication is busy or intermittent (disconnected).
 - 2.4.2.5. Automatic transfer of event clips to central host (VCC) for analysis and storage even under conditions when the connection has been temporarily lost during the transfer of the event clips with loss on neither frames nor video quality.
 - 2.4.3. Live Mode – On demand video streaming from the RVE to the VCC or directly from an IP camera or video server to the ActiveX control (requires TCP/IP network).
 - 2.4.3.1. Supports streaming from the RVE to the VCCover low bandwidth networks at rates as low as 2400 baud.
- 2.5. All RVE video modes will support:
 - 2.5.1. Configurable resolution, frame rates, and quality parameters.
 - 2.5.2. Optional time stamping embedded within the video stream.
 - 2.5.3. Configurable auto file deletion time period (# days to keep).
 - 2.5.4. Optional backup storage to allow additional removable (on the fly) or TCP/IP network storage of DVR files.

- 2.6. All RVEs will support either IP or Analog cameras. For IP, each RVE will support any compatible IP camera requiring either JPEG, MJPEG or MPEG-4 streaming capability. For IP cameras, the RVE shall support the following event detection methods:
 - 2.6.1. External Trigger - digital events triggered and collected external to the camera – Example: loss of video of one camera can trigger a PTZ operation. and clip generation of another camera.
 - 2.6.2. Digital Input trigger wired to the RVE I /O module, Modbus TCP Ethernet I/O module or an Axis IP camera.
 - 2.6.3. Audio Event trigger from an Axis IP camera with filter levels.
 - 2.6.4. Motion detection trigger from an Axis IP camera (with include and exclude zones).
 - 2.6.5. “No Video” or cable disconnect trigger.
 - 2.6.6. Tamper event trigger from an Axis IP camera.
- 2.7. All RVE systems shall support the generation of two types of “events”.
 - 2.7.1. Security Events - A security event can be triggered by any of the 12 digital inputs or by Longwatch video analytics motion detection or Axis IP video analytics of objects in any of the video streams. Upon detection of a security event, the RVE system supports:
 - 2.7.1.1. Triggering any of the 4 Digital Outputs.
 - 2.7.1.2. Creation of event clip data one or more, and as any as 4 video cameras.
 - 2.7.1.3. Trigger a defined notification rule (see section 3.2).
 - 2.7.2. Maintenance Events – The RVE shall support the generation of “maintenance” events for the following conditions:
 - 2.7.2.1. Power failure and restart of the RVE.
 - 2.7.2.2. Communications lost between the RVE and VCC.
 - 2.7.2.3. Health of the hardware or software that may effect system operation.
 - 2.7.2.4. Trigger of a defined notification rule (see section 3.2).
- 2.8. All RVE systems shall support the ability to arm and disarm the system from a hardwired input, from a keypad, a card reader, remotely from the HMI or remotely from the Longwatch web interface. The system shall support the automatic re-arming of the system based on either time of day or based on a length of time that the system was disarmed.

- 2.9. All RVE systems shall provide LATCHED event status. That is, if an event on a discrete input, video camera event, or access reader or keypad is triggered, this event is LATCHED in a separate status word available to the host system. This LATCHED status will require operator acknowledgement of the alarm before being cleared. The LATCHED status will be triggered and maintained even if there is a loss in communication between the host and remote.
- 2.10. All RVE systems shall support the ability to perform video analysis to create a security event (as noted above) based on object detection within a video image for any of 4 analog cameras. The user shall be able to specify:
 - 2.10.1. Sensitivity to changes in brightness.
 - 2.10.2. Sensitivity to changes in color
 - 2.10.3. Sensitivity to the size of the detected object
 - 2.10.4. In addition, the system shall perform continuous learning of the scene so as to minimize false alarms due to gradual changes in brightness.
- 2.11. All RVE systems can be centrally configured and managed with support for remote redeployment of all parameters. Furthermore, local configuration should be allowed through a local web browser to the RVE for maintenance purposes and/or initial installation. The LVS shall provide a means to upload any local configuration changes to the central configuration system.
- 2.12. All RVE systems will provide a local configuration and diagnostics web user interface accessible via a portable laptop with a direct Ethernet or wireless Ethernet connection. This UI will allow for:
 - 2.12.1. Local configuration of all modes of operation
 - 2.12.2. Configuration of local TCP/IP settings.
 - 2.12.3. Live video screens updating at 10 frames / second for camera tuning
 - 2.12.4. System time settings including local time zone setting
 - 2.12.5. File transfer of stored DVR files to the laptop or USB storage device
 - 2.12.6. Playback of DVR files within a browser
- 2.13. The RVE shall support the ability to easily transfer collected DVR files from the RVE to a USB storage device by simply inserting the USB storage device into the RVE without a need for any user interaction.
- 2.14. The RVE system shall support the transmission of events, event clips, and on-demand live feed to the host computer for operator analysis and long term event storage over any of the supported network protocols.
- 2.15. The RVE system shall support the transmission of DVR video to the host computer over TCP/IP networks.

3. The MICRO system shall incorporate the same operational features as section #2 with the following hardware characteristics:
 - 3.1. Support for 2 cameras.
 - 3.2. Support for external Modbus TCP Digital I/O with 8 Digital Inputs and 4 Digital Outputs.
 - 3.3. 1 Master Arm / Disarm Digital Input.
 - 3.4. Permanent solid state based storage of 4GB (expandable).
 - 3.5. RS232, USB, and Ethernet access ports.
 - 3.6. Optional (3) Serial Card Reader.
 - 3.7. Optional keypad.
 - 3.8. Temperature range of -40 to +70 Deg Celcius.
 - 3.9. Typical power consumption of 9 Watts.
4. The LVE system component shall support all operation features in section #2 along with the following extensions:
 - 4.1. The LVE shall support running on Windows XP Professional or Windows 2003 Server Operating Systems.
 - 4.2. Multiple LVE instances shall be able to be installed on the same PC.
 - 4.3. The LVE shall support up to 12 IP Cameras per instance.
 - 4.4. The LVE shall support up to 16 Access points (readers / keypads)
 - 4.5. The LVE shall support up to 16 Digital I/O from a Modbus TCP compatible I/O Module.
 - 4.6. The LVE shall support 30 frames per second of MPEG-4 streaming.
 - 4.7. The LVE shall support up to 150 frames per second overall using a 2.4 GHz Pentium 4 CPU
 - 4.8. The LVE shall support 1280 by 1024 high definition resolution for video archiving with event clips and live mode of 640 by 480 resolution.
5. The LVS shall have a central host computer consisting of the Video Control Center. The VCC should have the following characteristics.
 - 5.1. A Communications Manager that can support up to 64 remote RVEs, Micros, or LVEs (Video Engines) simultaneously. Support for both high and low bandwidth communication protocols including TCP, UDP, SIO (Serial I/O), Allen Bradley DF1, Modbus RTU, Modbus TCP, and Bristol Babcock BSAP over Public Switched Telephone Network lines, also known as POTS (plain old telephone service), radios, high-speed ISDN/DSL, cellular networks, satellite or internet communications.

- 5.1.1. The Communications Manager shall provide for the collection and storage of events and event clips from Video Engines as well as retrieving and sharing of any of the Video Engines Live mode streams.
 - 5.1.2. The Communications Manager shall provide for the retrieval of DVR video from any of the Video Engines when using a TCP/IP network.
 - 5.1.3. The Communications Manager shall support access to the live video stream from multiple clients in two modes.
 - 5.1.3.1. Guard Tour Mode – in this mode the VCC will periodically (configurable) request a snapshot of a camera to be cached in the VCC.
 - 5.1.3.2. Live Feed Mode – in this mode the VCC has received a client request to stream video as fast as the given network connection can support or as fast as the system is configured.
 - 5.1.4. The Communications Manager shall archive all security events received from the Video Engines into a central event database.
 - 5.1.5. The Communications Manager shall also generate “maintenance” events when communication is lost to a Video Engine or if any system is rebooted (Video Engine or VCC) indicating possible power failure and disrupted operations.
 - 5.1.6. The Communications Manager shall provide support for deploying to or uploading from a Video Engine.
 - 5.1.7. The Communications Manager shall support the automatic time synchronization of all video collection devices (Video Engines) to prevent time drift.
- 5.2. A Notification Manager that shall support the ability to define multiple notification rules consisting of a sequence of one or more contacts and executed when a security or maintenance event occurs.
- 5.2.1. The Notification Manager shall support text based email notification with support for event description and context hyperlinks capable of playing back the event’s associated video clips.
 - 5.2.2. A notification rule shall consist of a list of contacts to be notified with support for auto incrementing to a new set of contacts if an event is not acknowledged within a configured time period.
 - 5.2.3. The Notification Manager shall support remote email acknowledgement
 - 5.2.4. The Notification Manager shall support the attachment of the event video clip associated with the security event. This clip shall be playable by a standard video capable phone.

- 5.3. A UI Manager that shall provide a web-based interface for Configuration of the system as well as a Runtime user interface.
 - 5.3.1. The Configuration UI shall provide four views, the Event View, the Diagnostics View, the Live View, and the Config View.
 - 5.3.1.1. The Event View shall provide access to all maintenance and security events detected by the Longwatch system (VCC and all Video Engines). The Event View shall support:
 - 5.3.1.1.1. Filtering options including filtering by time/date and duration, event source (Unit or VCC), event source type (hardware, video, system), event category, acknowledge status.
 - 5.3.1.1.2. The ability to selectively playback any event video clip created in the system.
 - 5.3.1.1.3. Acknowledgment of a single event or the currently viewed page of events.
 - 5.3.1.1.4. Page based scrolling to all alarms specified by the filtering parameters.
 - 5.3.1.2. The Diagnostics View shall provide live status of each of the Video Engines, messages sent/received, as well as time of last received message.
 - 5.3.1.3. The Live View shall provide access to any of the Video Engine's cameras with the ability to select any camera and start live streaming or Guard Tour video modes.
 - 5.3.1.4. The Config View shall provide the ability to create, edit, deploy, and upload all Video Engine and VCC configuration parameters.
 - 5.3.2. The Web based Runtime UI shall provide an operator level user interface to provide runtime operation of the camera and event system. The Web based Runtime UI is hereinafter referred to as the Longwatch Viewer or LV. The Longwatch Viewer shall have the following key requirements:
 - 5.3.2.1. The LV shall provide access to all cameras via a web page with capability to navigate the cameras by Longwatch server (Video Engine) as well as the ability to group cameras into user configurable "Views" of cameras from different servers using simple click and drag and drop interface. Optionally, loading a new View will cause the trend chart to display a configured group of tags.
 - 5.3.2.2. The LV shall provide the ability to show cameras in either Tour, Live, DVR Playback, or Event Clip playback modes.

- 5.3.2.2.1. DVR playback mode shall support distributed DVR Playback allowing direct access to the collected DVR files stored on the Micro/RVE/LVE.
- 5.3.2.2.2. DVR playback mode shall support the following UI operations (PLAY,PAUSE,FORWARD, REVERSE, NUDGE, GOTO DATETIME, GOTO NEXT/PREVIOUS EVENT).
- 5.3.2.2.3. DVR playback mode shall support the concept of a central DVR and Event Clip Archive.
- 5.3.2.2.4. DVR playback mode shall provide the ability to playback video from the distributed LVE/Micro/RVE without the need for a central archive.
- 5.3.2.3. The LV shall provide 4 video matrix layouts (single camera, strip mode, 4 camera mode, and all camera dynamic layout mode).
- 5.3.2.4. The LV shall provide a tabbed area that will display Longwatch Event View interfaces as well as a means to extend the area to bring in external data to support additional “snap-on” applications to integrate process, production, or business information with collected video. The tabbed areas shall provide the capability to:
 - 5.3.2.4.1. Add and remove tabs by editing a simple XML file.
 - 5.3.2.4.2. Insert Trend Data and time synchronization between the trend data scrolling and DVR video playback. (Canary Labs Trending)
 - 5.3.2.4.3. Insert web pages, both user created and external web sites.
 - 5.3.2.4.4. Insert SQL query based data from any SQL capable database and automatic association of DVR playback to this data.
- 5.3.2.5. The LV will contain standard navigation buttons for DVR operations as well as next and previous event buttons to quickly change both the time and cameras based on events.
- 5.3.2.6. The LV and system shall support a means for the user to request clip for a camera on demand by user

- 5.3.2.7. The LV shall provide a means to lock the definition of View and Chart Group to prevent operators from changing this definition.
 - 5.3.3. The UI Manager shall not require IIS (Microsoft Internet Information Server) or any other 3rd party web server application software, but can integrate into it if available.
- 5.4. A new product offering called the “Video Historian”. The Video Historian shall provide the following capabilities.. In addition to these capabilities, the LVS shall support installation and licensing support for the Video Historian.
 - 5.4.1. The Video Historian shall provide support for automatic association of DVR playback to user data stored in a SQL database (Process Tab and backend dynamic camera association).
 - 5.4.2. The Video Historian shall provide per client licensing.
 - 5.4.3. The Video Historian shall provide a SQL API Toolkit to allow users to query the Longwatch database.
 - 5.4.4. The Video Historian shall provide support for Trend Data integration and time synchronization between the trend data scrolling and video playback. (Canary Labs Trending)
 - 5.4.5. The Video Historian shall provide the ability to access a list of event clips based on process data context (BatchID, phase, equipment association, alarm point) via the use of 5 user configurable camera attributes. These attributes can be manual entered or dynamically changed via OPC or the LV to allow process data to be associated with an event clip.
- 5.5. The VCC shall provide a set of plug and play components, using accepted industry standards, to allow video streams, clips, and events to be integrated with the existing process control and monitoring system. These components include:
 - 5.5.1. The LVS shall support standard Windows based HMI packages including but not limited to, iFIX from GE Fanuc, Intouch from WonderWare, and RSView from Rockwell.
 - 5.5.2. The LVS shall support the sharing of any one camera video stream or event clip with multiple clients and/or HMI SCADA systems or HMI displays.
 - 5.5.3. The LVS shall support the ability of the HMI to generate alarms based on security and maintenance events generated by the LVS via an industry standard OPC server. The OPC server shall support the ability to:
 - 5.5.3.1. Supply both direct and latched event status for each of the DIs or video detection input statuses on any of the deployed Video Engines.
 - 5.5.3.2. Supply an ANY alarm and ANY latch alarm status.

- 5.5.3.3. Clear the input latched status.
- 5.5.3.4. Set to “force” the output state of any of the Digital outputs on the Video Engine.
- 5.5.3.5. Supply diagnostic values on the communication status of the Video Engine and bandwidth utilization.
- 5.5.4. A single camera view component utilizing ActiveX and / or HMI object technology to provide for the integration of a video camera’s guard tour stream, live stream, event clip or DVR stream display embedded directly in an HMI screen. This video camera view shall support:
 - 5.5.4.1. Resizable camera windows embedded in the HMI to display a specific camera’s guard tour stream, live stream, event clip, or DVR stream. Scaling of the image display should be controllable to either fixed size or best fit.
 - 5.5.4.2. Cycle through a configurable set of Video Engine/camera combinations at a control switching rate with the ability to freeze cycling and switch from guard tour, live, event clip, or DVR streams.
 - 5.5.4.3. Support scripting access to all properties for specific site / display characteristics.
- 5.5.5. An event view component to provide a means for the HMI to display and query the event history stored in the VCC system with fully query and filtering capability as well as the ability to playback an event’s associated video clip.
- 5.6. Access Control
 - 5.6.1. Centralized Administration
 - 5.6.1.1. All changes (such as access for new or terminated employees, temporary workers, or contractors) are made from a central location and deployed to each remote location.
 - 5.6.1.2. Entry into remote locations can be granted in real time from central location.
 - 5.6.1.3. Central operators have a comprehensive view of the status of all remote locations.
 - 5.6.1.4. Alarm and event history is recorded centrally for forensic or auditing purposes.
 - 5.6.1.5. Assigned access cards are unique to each user and can be configured to control, monitor, and report on access to specific buildings, doors, or other assets.

- 5.6.1.6. Remote site security can be configured for two levels of security - badge and user password validation.
- 5.6.1.7. The remote equipment and logic continues to operate without the central location during periods of lost communications.
- 5.6.2. Communication to access control system
 - 5.6.2.1. Leverages existing remote PLC/RTU or wireless TCP/IP communications network if present.
 - 5.6.2.2. Common PLC protocols such as Modbus, BSAP and DF1 are supported.
 - 5.6.2.3. System is operable on virtually any communications media from telephone lines to fiber-optic cabling, including radios, frame relay, satellite and cellular connections.
 - 5.6.2.4. Communications are uniquely designed for low bandwidth (9600 baud) and scales to high bandwidth LAN/WAN networks.
- 5.6.3. Integrated Access Control and Video surveillance
 - 5.6.3.1. Access control events can be synchronized with video clips to track access and verify each entry.
 - 5.6.3.2. Access control events such as Door Open, BadBadge, and Tamper event can trigger Video clip and PTZ operations.
- 5.6.4. Access Control integration into SCADA
 - 5.6.4.1. Allows the use of existing SCADA/HMI to manage process alarms, security alarms, and access control in the same environment.
 - 5.6.4.2. Tools such as OPC, ActiveX controls and modular web pages can be integrated into existing SCADA screens to provide real-time visibility to remote doors and alarm status.
 - 5.6.4.3. Support integration of an event history showing all access events along with associated video clips should be easy integrated into an HMI graphic.
- 5.6.5. Readers
 - 5.6.5.1. Support HID proximity cards (26-bit and Extended modes)
 - 5.6.5.2. Support persistent storage of deployed cards that would allow for full reader operation in the event network connection is lost.

5.6.5.3. Integration with a numeric keypad to support user specific, two level verification of card and associated password.

5.7. Pan, Tilt, Zoom

- 5.7.1. PTZ operations shall support PELCO-D compliant analog cameras.
- 5.7.2. PTZ operations shall support Axis IP PTZ cameras.
- 5.7.3. PTZ operations shall support IV&C PTZ cameras.
- 5.7.4. The system shall support 9 named presets per camera.
- 5.7.5. The system shall support the ability to trigger a preset from a digital input (motion sensor), video analytic event, card reader event, Axis camera event, remote GOTO command from the host system, or via OPC.

5.8. Security

- 5.8.1. The system shall support the ability to prevent access to the web based configuration by using Windows Integrated system security.
- 5.8.2. The system shall support the use of standard Windows domain or system user accounts as authentication and be able to granted permission to configure and /or monitor the system events and video.
- 5.8.3. The system shall support optional 128 bit TCP Encryption between the central station and all remotes. Furthermore, the system shall also enforce support data encryption between the central station and all LAN clients (video streaming and OPC access).

5.9. Streaming

- 5.9.1. The system shall support the ability to publish a JPEG and MJPEG video stream of any of the remote Video Engine's cameras to allow video integration into 3rd party in-plant security products.